Information Hiding Techniques on Various Medium

Ramya.S , Poorani.G, Priya.J, Brindha.M

Abstract— **Various steganography algorithms in different cover medium are reviewed here. By combining cryptography and steganography techniques, security is improved highly when compared to the information hiding process with one security techniques. The data can be hidden in any carrier like text, audio, images and video. Embedding capacity and noise ratio are used as a performance measure.**

Index Terms— **steganography, cryptography, embedding capacity,performance measure.**

I. INTRODUCTION

Sharing information over networks has increased over many years. To prevent our secret information from intruders two security techniques have been used broadly over the internet. Two security techniques are cryptography and steganography. In cryptography technique, the secret message is not concealed, but the existence of the message is covered and thus intruders are confused while extracting the secret data. The secret texts are concealed using the cipher algorithm by encrypting and decrypting the message. Private Key and public key are used for encryption and decryption, the private key which is known only to the sender and receiver and the public key is kept common. The most common algorithms used in cryptography are data encryption standard, advanced data encryption and hash algorithm and this technique is used for confidentiality, authentication and security purpose.

But cryptography technique is alone not enough to provide full security, thus steganography is concept is also used. Steganography is the art of science where the secret text or data are hidden in cover medium and that cover medium is communicated over unprotected networks. The secret message will be invisible to the intruders, a secret key is used between the sender and receiver and with the help of that secret key the data can be retrieved at the receiver side. Steganography concept comes under information hiding techniques, other information hiding techniques are watermarking and covert channel. The secret data being embedded can be of text, images, audio and video and the cover medium can also be text, images, audio and video. In video the data are stored in frames. Least significant bit is the most common hiding algorithm, many algorithms developed over many years. To improve the security, the data are encrypted before embedding into the cover medium.

Compression technique is used to reduce the size of the embedded carrier file, thus the network traffic can also be minimized. Lossless and lossy are the two types of compression techniques, lossy compression is used for images and audio and lossless compression is used for text.

II. LITERATURE REVIEW

Cryptography and steganography are the two most widely used techniques for secure information sharing through any communication channel. Palesh.et.al [1] proposed a format based pure text steganography algorithm where both encryption and decryption are carried out through DES(data encryption standard). First the data or messages to be embedded are encrypted using 16- digit hexadecimal key, then the cipher text value is taken for the key and the position of each character and frequency of characters are calculated. By comparing the character position in over text, equivalent ACII for the character position is obtained. Alphanumeric puzzle is generated which contains two parts, characters that conceal the messages are in the first part and positions of characters are in the second part. At the last the puzzle is added at the end of cover text. The reverse process is carried out for the extraction.

Odeh. et. al [2] to avoid suspicion and attacks over the internet, a novel secure algorithm has been proposed in which the data or secret data hide inside the document files. First a symbol table is produced and the embedded data are compared to the representative symbols maximally four bits are embedded between letters without affecting the size of the word file and the content of file. Mainly right remark, left remark, zero width joiners, and zero width non joiner are used for embedding process.

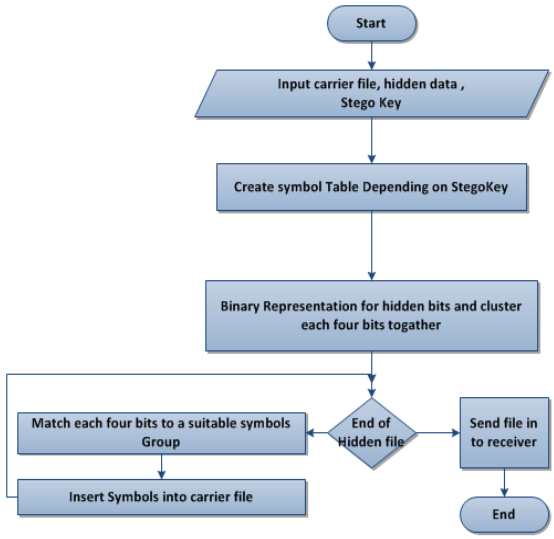

Fig 1: Data hiding algorithm

In most of embedding techniques the cover medium with any size are taken without considering the size of secret bits and image content. Luo.et.al [3] proposed an algorithm where a region for embedding has been chosen with relation of secret bits, if the embedding rates are lower then the sharper edge is selected and if the embedding rates are higher then more edge regions are selected for embedding process. This algorithm is compared with six steganography algorithms such as PVD, LSBM, LSBMR, IPVD, AE-LSB and HBC. When comparing with other algorithm, this approach shows that visual quality and security are improved. In embedding stage some parameters are identified before the region selection.

parul.et.al [4] proposed AWPAS(adaptive wavelet packet based audio steganography) algorithm where the secret bits are hidden in audio. The embedding process contains various steps, as first step wavelet packet decomposition is carried out in which audio signals are decomposed. To reduce the noise ratio in stego audio, high frequency bands are selected for embedding, here HLH band is used for better performance. In the second step, the co-efficient of the selected bands are converted into 2 dimensional matrix by binary mapping and the blocks for embedding data are selected using pseudo random sequence. The secret data are encrypted before embedding process. Patter classification and pattern modification are done as third step, for embedding data . At last inverse wavelet packet is applied on modified packet co-efficient to obtain stego audio file. AWPAS algorithm is tested with different audio files.

Balaji.et.al [5] proposed an algorithm where the secret information data is hidden inside the video. In existing algorithm the information is hidden in the sequential frames. Here in the proposed algorithm, the information are stored in the random frames. Index is created for secret data and then that index is placed in video frames. The frame which does not contain secret information is used for storing some random data. This process improves the security. The same index is used for the extraction process. The proposed system contains 3 phases such as analyzing the video, determination of index frame and its data and determination of frames for secret data. The advantage of balaji.et.al algorithm are less computational time and highly securable.

Karais.et.al [6] proposed steganography on medical images and two methods such as LSB based on fuzzy and similarity are used. In similarity based LSB, similarity between adjacent pixel values are seen. If the similarity pixel value is higher than threshold, then they are selected to hide messages. Patient's medical information and doctors comments are hidden inside the image for security purposes**.** EEG and magnetic resonance images are used for embedding purpose. The comparison study is done and the various performance measures such as MSE, SSIM, PSNR and UQI are taken for measuring the quality of stego image.

Vidhya.et.al [7] proposed a steganography algorithm using Malayalam text. Here custom Unicode is used for encoding the original message to Malayalam. Two matrices are used for indexing English and Malayalam. Then Unicode extraction step helps to find the corresponding English text for Malayalam text. Before embedding the original secret message is mixed with Malayalam text for security purpose. The comparison study on proposed algorithm achieves presion rate of 0.95 and decoding is 0.81.

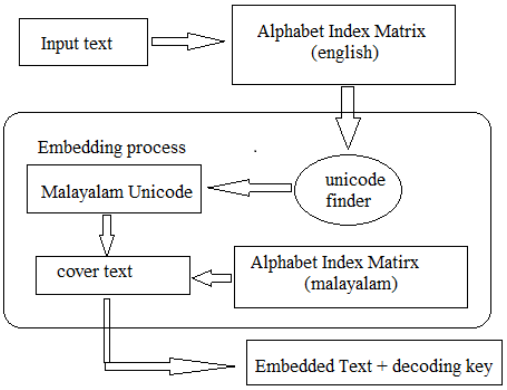

Fig 2: Vidhya.et.al [7] algorithm

Diqun.et.al [8] proposed a data hiding algorithm where the secret information are hidden in mp3. In this paper window switching method is used for encoding. Distortions are caused during the embedding process are automatically controlled by distortion adjustment mechanism. Operations are carried out on consecutive frames of mp3 audio. Window switching technique is

used to avoid pre-echo distortions. This method provides better solution when comparing to other audio steganography. In future this window switching can be applied to other audio formats like MPEG.

Most common steganography direct LSB algorithm is not suitable for the audio steganography. Dulal.et.al [9] proposed a multi threshold based audio steganography where the threshold value is determined from the error criterion, which limits the no. of secret bits per sample of audio signals. The changes in each audio sample are focused to state the threshold value. The implementation, first the audio sample based on threshold limit is selected. Chaotic order is also proposed and in this order the samples are choose from selected samples. Then the samples are adjusted to reduce the error. This embedding process is carried out in WAVE audio format. The size of audio documents preferred here are 8 bits per sample and 16 bits per sample.

Amritha sekhar.et.al [10] proposed network steganography method where the secret messages are embedded in the host medium and the host medium may be of Skype, bit torrent, goggle suggests and WLAN's. Instead of internet services, protocols are also used as carriers. In this paper network protocols using PRNGs is used for steganography. The sender generates key and places in the header of the file and to confuse the intruder's fake key is used. The secret data are encrypted and embedded in the video file; then again the resultant file is encrypted and compressed. At the receiver side the secret bits are decrypted and finally the key decrypted from header is also used.

III. CONCLUSION

Information security techniques such as cryptography and information hiding are reviewed. Steganography concept has been used to prevent secret data communicated over unprotected networks. Intruders find difficult to extract the data from the carrier when both cryptography and information hiding techniques are used. Embedding capacity various for different host medium.

REFERENCES

[1] Md.Palash Uddin, M.Saha, S.J. ferdousi, M.I. Afjal, Md.Abu Marjan,"Developing An Efficient Solution To Information Hiding Through Text Steganography Along With Cryptography",in 9th international forum on strategic technology(IFOST), oct 21-23,2014,cox's Bazar,Bangladesh.
[2] A. Odeh, K.Ellerithy, M.Faezipour,"Steganography In Text By Using MS Word Symbols", in proceedings of 2014 zone 1 Conference of American Society for engineering Education(ASEE ZONE 1).
[3] W. Luo, F. Huang and J. Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE transactions on information forensics and security, vol. 5, no. 2, June 2010.
[4] Parul Shah, Pranali Choudhari and Suresh Sivaraman, "Adaptive Wavelet Packet Based Audio Steganography using Data History", IEEE , Dec 2008.
[5] R. Balaji and G. Naveen, "Secure Data Transmission Using Video Steganography".
[6] R. Karakıs, I. Guler, I. Capraz, E. Bilir, "A Novel Fuzzy Logic-Based Image Steganography Method To Ensure Medical Data Security", Computers in Biology and Medicine, http://dx.doi.org/10.1016/j.compbiomed.2015.10.011.
[7] Vidhya P.M and Varghese Paul, "A Method for Text Steganography Using Malayalam Text", International Conference on Information and Communication Technologies (ICICT 2014), Procedia Computer Science 46, pp. 524 – 531, 2015.
[8] Diqun Yan, Rangding Wang, Xianmin Yu and Jie Zhu, "Steganography for MP3 audio by exploiting the rule of window switching", Computers & Security 31, Elsevier, pp. 704-716, 2012.
[9] Dulal C. Kar and Clifton J. Mulkey, "A multi-threshold based audio steganography scheme", Journal of information security and applications, Elsevier, pp. 1-14, 2015.
[10] Amritha Sekhar, G.Manoj Kumar and M.Abdul Rahiman, "A Novel Approach for Hiding Data in Videos Using Network Steganography Methods", 4thInternational Conference on Eco-friendly Computing and Communication Systems, Procedia Computer Science 70, pp. 764 – 768, 2015.
[11] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray scale images," *IEEE* Multimedia, vol. 8, no. 4, pp. 22–28, Oct. 2001.
[12] J. Harmsen and W. Pearlman, "Steganalysis of additive-noise modelable information hiding," Proc. SPIE Electronic Imaging, vol. 5020, pp. 131–142, 2003.
[13] A. D. Ker, "Steganalysis of LSB matching in grayscale images," IEEE Signal Process. Lett., vol. 12, no. 6, pp. 441–444, Jun. 2005.
[14] J. Zhang, J. Li, and L. Zhang, "Video watermark technique in motion vector," in Proc. XIV Symp. Computer Graphics and Image Processing, Oct. 2001, pp. 179–182.
[15] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

AUTHOR PROFILE

Ramya.S received a bachelor degree in computer science engineering from Avinashilingam university and is pursuing master in computer science engineering from Sri Ramakrishna Institute of Technology. Her area of interests include image processing and data structure.

Poorani.G received a bachelor degree in computer science engineering from Avinashilingam university in

2014 and pursuing master in computer science engineering from Sri Ramakrishna Engineering College. Have published 1 journal and area of interest is image processing.

Priya.J received a bachelor degree in computer science engineering from Kathir College of Engineering in 2014 and pursuing master in computer science engineering from Sri Ramakrishna Institute of Technology. Area of interest are cryptography and image processing.

Brindha.M received a bachelor degree in computer science engineering from Knowledge Park for Engineering and Technology in 2014 and pursuing master in computer science engineering from Sri Ramakrishna Institute of Technology. Area of interest are software engineering and image processing.